Siber zorbalığa karşı tedbir almalıyız

Fatih Yardım

Sanal dünyanın kâbusları arasında siber zorbalık üst sıralara giderek tırmanıyor. Sanal dünyada yaşanan şiddetin en fazla gençleri ve çocukları tehdit ettiği belirtiliyor. 6-12. sınıf okuyan bireylerin neredeyse yarıya yakınının en az bir kez siber zorbalığa maruz kaldıklarına dikkat çeken uzmanlar, bu durumun üzüntü, korku, öfke, kaygı, akademik başarıda düşme şeklindeki sonuçlarına dikkat çekiyor. Siber zorbalık genellikle tehdit ya da şantaj içeren bir mesaj, gerçek ya da gerçek dışı dedikoduların online platformlarda yayılması, ifşa ve benzeri eylemler olarak tanımlanıyor.

Burada, siber güvenlik alanında danışmanlık, teknoloji tedariki ve saha hizmetleri sunan Innovera'nın konuya ilişkin önerilerini vermek istiyorum. Aileleri özellikle çocukların ve gençlerin karşı karşıya kalabileceği siber zorbalık vakalarına karşı evdeki tüm kullanıcıların aktif katılımıyla hayata geçirilmesi gereken kurallar şöyle sıralanıyor:

■ Bilgisayarım, akıllı telefonum ya da diğer elektronik cihazlarım aracılığıyla beni rahatsız eden bir kişi veya durum olursa derhal bunu ailemle paylaşacağım.

■ **Aile büyüklerimden müsaade almadan kendime veya başkalarına ait hiçbir fotoğrafı, videoyu ve görsel materyali sosyal ağlarda ya da diğer online platformlarda paylaşmayacağım.**

■ Anne ve babamın haberi ve izni olmaksızın, tanımadığım kişilerle online olarak görüşmeyeceğim. Böyle kişilerle akıllı telefon aracılığıyla iletişim kurmayacağım.

■ **Beni tehdit veya rahatsız eden, dalga geçen ya da kendimi kötü hissetmeme neden olan her türlü mesajı önce anne ve babama bildireceğim. Bu tür mesajları almamın kesinlikle benim suçum olmadığının farkında olacağım.**

■ Kendim de bir siber zorba olmayacağım! Sosyal medya, e-posta veya akıllı telefon gibi dijital iletişim araçlarını kullanarak kimseyi incitecek sözler yazmayacak, dedikodu yapmayacağım.

■ **Ev adresimizi, telefon numaramı, aileme ait iş yeri ve telefon bilgilerini onların haberi ve izni olmadan kesinlikle hiç kimseyle paylaşmayacağım.**

■ Bilgisayarımda, sosyal medyada ve mobil cihazlarımda kullandığım şifreleri ailem dışında kimseye söylemeyeceğim. Bu şifreleri isteyen bir arkadaşım bile olsa, hemen anneme veya babama haber vereceğim.

■ **İnterneti ve sosyal medyayı kullanacağım zamanı, ziyaret edebileceğim web sitelerini ve uygulamaları aile büyüklerimle birlikte belirleyeceğiz.**

■ Bilgisayarıma, akıllı telefonuma ya da diğer elektronik aygıtlarıma herhangi bir dosya, uygulama veya görüntü indirmeden önce mutlaka anne ve babamın iznini alacağım.

İşte bunları uygulayabilirsek, internette yaşayabileceğimiz kâbuslardan kurtulabiliriz.

Aile boyu güvenli internet için 5 ipucu

HER aygıtın birbirine bağlı olduğu dijital bir dünyada yetişen çocuklar, oyun ve eğlenceyi de yine internete bağlı cihazlarla elde ediyor. Facebook oyunlarından Roblox maceralarına kadar, çocukların kullandıkları platformlar hem onları hem de aileleri zararlı yazılımlara ve virüslere karşı savunmasız bırakıyor. Üstelik tanımadıkları kişilerle online olarak iletişim kurmanın riskleri de her geçen gün artıyor. Aile içinde internet kullanımını daha güvenli kılmak için halen yapılacak çok şey olduğunu dile getiren McAfee EMEA Tüketici Grubu Başkanı Jessica Brookes, "Her şeyin birbirine bağlı olduğu bir dünyada kıymet verdiklerini koruyabilmek çok önemli" dedi. Her bireyin, diğerini eğitmekle yükümlü olduğunu ifade eden Brookes, "Yaşadığımız bağlı dünyada insanların karşılaştığı mevcut tehditlere karşı kendimizi korumak için iş birliği yapmalı ve sahip olduğumuz bilgi birikimini paylaşmalıyız" diyor.

McAfee'nin ailelerin siber emniyetini sağlamak amacıyla paylaştığı ipuçları ise şöyle sıralanıyor:

Tıklamadan önce iki kez düşünün: Siber suçluların cihazınızı ele geçirmesinin en kolay yolu kötü amaçlı bir bağlantıya tıklamanızı sağlamaktır. Beklenmedik bir bağlantı gördüğünüz veya aldığınız zaman tedbirli davranın.

Yazılımınızı güncel tutun: Bilgisayarınız, akıllı telefonunuz, oyun konsolunuz ve hatta kullandığınız drone; yazılımınızı her aygıtınızda güncel tutmaya özen gösterin. Üretici firmalar her yeni cihaz güncellemesinde bir dizi güvenlik açığını kapatır, bu nedenle en güncel sürümü yayımlandığı anda yüklemeniz faydalı olacaktır.

Wi-Fi erişim noktalarına dikkat edin: Siber suçlular genelde normal görünen sahte Wi-Fi erişim noktaları kullanarak, tarayıcınıza erişim sağlıyor. Herkese açık (public) bir Wi-Fi kullanıyorsanız, online alışveriş ve bankacılık uygulamalarından uzak durun. Mutlaka bu ağlarda alışveriş yapmanız gerekiyorsa, McAfee Safe Connect gibi ağ trafiğinizi gizleyen bir VPN kullanın.

İpleri elinize alın: Her üretici güvenliğe aynı ölçüde özen göstermiyor; özellikle de internete bağlanabilen oyuncaklar gibi aygıtlar söz konusu olduğunda. Bu nedenle bu gibi ürünleri satın almadan önce, daha önce bir güvenlik zaafiyeti ortaya çıkmış mı araştırın.

Ev ağınızı koruyun: Bağlı cihazlarınızın tamamını ve ev ağınızı antivirüs programı ile koruyun. McAfee Secure Home Platform da bunlardan birisi. Bu çözüm ile ağınıza bağlı cihazları görebilir ve bağlı tüm cihazları koruyabilirsiniz.

Dijital hayatınızı yedekleyin!

GÜNÜMÜZDE bir kişi ayda ortalama 10 GB veri üretmeye başladı. Resim, video, ses veya metin dosyaları, artık milyonlarca insanın gündelik hayatının birer parçası. Paradan daha kıymetli olabilecek fotoğrafların, kişisel verilerin silinmesi veya ulaşılamaz hale gelmesi, çok can sıkıcı olabilir. ESET uzmanları bu konuda yedekleme uyarısında bulunuyor. ESET, "Kurban olmaktan kaçınmanın en iyi yolu proaktif bir savunmadır. Verileri kendi eviniz gibi düşünün; alışverişe gittiğinizde kapıyı açık bırakmazsınız. Dizüstü bilgisayarların veya akıllı telefonların onarılamaz derecede hasar görmesi veya tehlikeye girmesi riskine karşı, verilerinizi harici sabit diskler gibi uzaktaki cihazlarla güvende tutun. Bu sırada, şifrelerinizi sık sık değiştirerek, yazılımın siber suçlulara karşı korunmasına yardımcı olun. Sürekli güncellenen proaktif bir güvenlik yazılımı kullandığınızdan da emin olun" açıklaması yaptı.

Panasonic'in yeni Toughbook'u

PANASONIC sağlamlaştırılmış ve ayrılabilen en yeni notebook modeli Toughbook CF-20'nin yeni modelini tanıttı. Panasonic Toughbook CF-20, 7. Jenerasyon Intel CoreTM vProTM işlemci kullanıyor. Açıklamaya göre, ikisi bir arada cihazların standart klavye alanında yer alan ve tek başına tableti 8,5 saat boyunca çalıştırabilen ikinci bir batarya sayesinde batarya ömrü 17 saate kadar uzayabiliyor. Ürünün, Windows Hello destekli ön kamerasının yanı sıra kızılötesi sensörü ve LED ekranıyla gelişmiş kullanıcı giriş güvenliği dikkat çekiyor. Bu özellikleri bir arada kullanabilen kullanıcılar, kendilerinin 3 boyutlu bir resmini oluşturduklarında, kullanıcı adı veya şifre bilgileri yerine kullanıcı girişi sırasında bu resim ile kendi yüzlerini eşleştirerek cihazlarını kullanabiliyorlar.

Fujitsu'dan sık seyahat edenlere

FUJITSU, sık seyahat edenler için tasarlanmış, ultra mobil dizüstü bilgisayarının geliştirilmiş versiyonu olan LIFEBOOK U938'i görücüye çıkardı. LIFEBOOK U938'in 8. nesil Intel Core vPro işlemciler, tam boyutlu bağlantı portları ve kurumsal sınıf biyometrik kimlik doğrulaması bulunuyor. 13.3 inç (33.8cm) ekrana sahip ürün, 15.5mm boyunda ve 920 gr ağırlığında. LIFEBOOK U938'un HDMI, USB türleri A ve C, sesli açılır kutu, SD ve akıllı kart okuyucu ve isteğe bağlı 4G / LTE'modülü seçenekleri var.

e-posta: yardimfatih@yahoo.com